The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
12/13/2011

SUBJECT:
Cumulative Security Update of ActiveX Kill Bits (MS11-090)

OVERVIEW:
Microsoft has released a security update which addresses vulnerabilities discovered in multiple ActiveX controls. Exploiting these vulnerabilities could allow an attacker to take complete control of an affected system. ActiveX controls are small programs or animations that are downloaded or embedded in web pages which will typically enhance functionality and user experience. Exploitation may occur if a user visits a web page, or opens an HTML-formatted email which is specifically crafted to take advantage of one or more of these vulnerabilities. Successful exploitation of any of these vulnerabilities could allow an attacker to gain the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:
Windows XP
Windows Server 2003

RISK:
Government:
Large and medium government entities: **High**
Small government entities: **High**

Businesses:
Large and medium business entities: **High**
Small business entities: **High**

Home users: High

DESCRIPTION:
The following vulnerabilities have been discovered in Microsoft products that utilize ActiveX controls. The vulnerability could allow an attacker to take complete control of an affected system.

Microsoft Time Remote Code Execution Vulnerability This vulnerability exists in the Microsoft Time component. Exploitation may occur if a user visits a web page, or opens an HTML-formatted email containing a specifically crafted ActiveX control.

Third Party ActiveX Kill Bits
Third party Active X controls for Dell, Hewlett Packard (HP) and Yahoo! have also been included in this security update to prevent the following ActiveX controls from being run in Internet Explorer:
The Dell ActiveX control relates to IT Assistant.
The HP ActiveX controls relate to Easy Printer Care Software and Photo Creative.
The Yahoo! ActiveX control pertains to pertains to Yahoo! CD Player.

RECOMMENDATIONS:
The following actions should be taken:

- Apply the security update provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Configure email clients to preview messages in plain-text format, rather than RTF or HTML format.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:
Microsoft:
http://technet.microsoft.com/en-us/security/bulletin/ms11-090

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3397

Security Focus:
http://www.securityfocus.com/bid/45631
http://www.securityfocus.com/bid/48680
http://www.securityfocus.com/bid/49100
http://www.securityfocus.com/bid/50970
http://www.securityfocus.com/bid/51011